A1

22. (Once Amended) A method for decrypting encrypted communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving from an originating node a multicast that includes encrypted data and an identifier;

identifying the identifier from the multicast;

sending a request that includes the identifier to an authoritative node for an encryption key used by the originating node to encrypt the encrypted data;

in response to the request to the authoritative node, receiving the encryption key; and

decrypting the encrypted data based on the encryption key.

A2

24. (New) A computer-readable medium carrying one or more sequences of instructions for facilitating secure communications among multicast nodes in a telecommunications network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;

in response to the first request,

storing the encryption key;

creating and storing an association between the encryption key and the identifier;

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier;

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key; and sending the encryption key to the at least one second node for use in decrypting the encrypted data.

25. (New) A computer-readable medium carrying one or more sequences of instructions for encrypting communications among multicast nodes in a telecommunications network, cause the one or more processors to carry out the steps of:

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier;

encrypting data based on the encryption key; and

multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.

A2

26. (New) An apparatus for facilitating secure communications among multicast nodes in a telecommunications network, comprising:

means for receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;

means for storing the encryption key, in response to the first request;

means for creating and storing an association between the encryption key and the identifier, in response to the first request;

means for receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier;

means for retrieving the encryption key, in response to the second request and based on the identifier included in the second request and the association between the encryption key and the identifier; and means for sending the encryption key to the at least one second node for use in decrypting the encrypted data, in response to the second request.

27. (New) An apparatus for encrypting communications among multicast nodes in a telecommunications network, comprising:

means for sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier;

means for encrypting data based on the encryption key; and

means for multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.

A2

28. (New) An apparatus for facilitating secure communications among multicast nodes in a telecommunications network, comprising:

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes;

in response to the first request,

storing the encryption key;

creating and storing an association between the encryption key and the identifier;

receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier;

in response to the second request,

based on the identifier included in the second request and the association between the encryption key and the identifier, retrieving the encryption key; and

sending the encryption key to the at least one second node for use in decrypting the encrypted data.

A2

29. (New) An apparatus for encrypting communications among multicast nodes in a telecommunications network, comprising:

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier;

encrypting data based on the encryption key; and

multicasting the encrypted data with the identifier to one or more receiving nodes, wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node and decrypt the encrypted data based on the encryption key.